UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
v.	)	21-cr-10104-PBS
VLADISLAV KLYUSHIN,	)	
Defendant.	)	

OPPOSITION TO DEFENDANT'S MOTION TO ACQUIT FOR IMPROPER VENUE

Over ten trial days, the jury heard extensive evidence that defendant Vladislav Klyushin—together with Ivan Ermakov, Nikolay Rumiantcev, and others—repeatedly targeted the computer network of Donnelly Financial ("DFIN") from a computer server located in Boston, Massachusetts. They accessed a Virtual Private Network ("VPN") on that Massachusetts server, and used the VPN to log into DFIN's network without authorization, using credentials stolen from a DFIN employee, Julie Soma. Once inside, they stole confidential and valuable financial information of DFIN's publicly-traded clients, which they directed DFIN's computers to download to the Massachusetts server. They ultimately viewed that MNPI in Russia and, in one of the most profitable hack-and-trade schemes in history, used it to reap approximately $90 million in insider trading profits. Based on that overwhelming evidence, and after being instructed that it must find venue for each of the four counts of the Indictment, the jury convicted Klyushin on each count.

Upon conviction, typical white-collar defendants file detailed post-trial motions, for judgment of acquittal under Rule 29 and/or a new trial under Rule 33. They contend, for example, that the government failed to prove the charged conspiracy beyond a reasonable doubt; that there was a prejudicial variance; that the evidence did not prove the defendant joined the conspiracy;

that the Court's evidentiary rulings or jury instructions were incorrect; and, in nearly every case, that the government failed to prove the defendant's criminal intent.

The defendant's Rule 29 motion makes none of these arguments. Instead, recycling an argument that the jury rejected, Klyushin asks this Court to reverse his four convictions on venue grounds. In essence, he contends that because other venues may also have been appropriate for this prosecution, he should not have been prosecuted here.

His motion is legally and factually without merit, and the Court should deny it. It ignores or barely references relevant law—including the standard applicable to a Rule 29 motion—cites precedent that courts in this and other Circuits have expressly rejected, and invokes a Department of Justice manual that confers on him no substantive or procedural rights. Not surprisingly, where he must both meet Rule 29's exacting standard and overcome the preponderance-of-the-evidence standard governing venue challenges, Klyushin cites no case in this District where a Rule 29 motion was granted on venue grounds.

His motion—which cites the trial record only twice—whistles past the venue evidence that the jury considered. That evidence and all reasonable inferences drawn from it, taken in the light most favorable to the government, easily permitted a rational jury to find venue by a preponderance of the evidence on each of the four counts of the Indictment. Finally, contrary to Klyushin's contention, there is no requirement in the First Circuit that venue in Massachusetts have been foreseeable to him (an issue the Court has already resolved), and Klyushin was brought directly to this District following his arrest in Switzerland, making "first brought" venue independently proper under 18 U.S.C. § 3238 as to each count of the Indictment.

LEGAL STANDARD

Rule 29 provides that "[a] judgment of acquittal should only be granted when the evidence

and all reasonable inferences to be drawn from the evidence, both taken in the light most favorable to the government, are insufficient for a rational factfinder to conclude that the prosecution has proven . . . each of the elements of the offense." *United States v. Pimental*, 380 F.3d 575, 584 (1st Cir. 2004). Because venue is not an element of any of the charges in the Indictment, the prosecution's burden, on Rule 29 review as at trial, is to show venue by a preponderance of the evidence. *United States v. Tang Yuk*, 885 F.3d 57, 71 (2d Cir. 2018); *United States v. Jones*, 302 F. Supp. 3d 752, 756 (W.D. Va. 2017). In assessing a Rule 29 motion, the court "do[es] not weigh the evidence or make any credibility judgments, as those are left to the jury." *United States v. Merlino*, 592 F.3d 22, 29 (1st Cir. 2010)). Rather, the court must "examine[] the evidence—direct and circumstantial—as well as all plausible inferences drawn therefrom, in the light most favorable to the [government]." *United States v. Meléndez-González*, 892 F.3d 9, 17 (1st Cir. 2018).

Rule 29 poses "daunting hurdles" for a defendant. *United States v. Hatch*, 434 F.3d 1, 4 (1st Cir. 2006) (further citations omitted); *see also United States v. López-Díaz*, 794 F.3d 106, 108 (1st Cir. 2015) (observing that it is "rare" for the court to determine under Rule 29 that the trial record "lacks sufficient evidence to support a guilty verdict"). "[I]t matters not whether [the defendant] can raise a plausible theory of innocence: if the record as a whole justifies a judgment of conviction, it need not rule out other hypotheses more congenial to a finding of innocence." *United States v. Manor*, 633 F.3d 11, 14 (1st Cir. 2011) (cleaned up).

As courts in this District have held in denying Rule 29 motions, this "daunting" standard is particularly so in the context of venue arguments. *See, e.g.*, *United States v. Foley*, 2013 WL 210187, *1 (D. Mass. Jan. 18, 2013) (Stearns, J.) (denying Rule 29 motion on venue grounds, explaining that the record is reviewed "in the light most favorable to the government," noting that venue "need only be shown by a preponderance of the evidence," and concluding that because,

under those standards, it was "reasonable to draw the conclusion" that the jury reached, the motion must be denied), *aff'd*, 783 F.3d 7 (1st Cir. 2015); *United States v. Harris*, 2012 WL 2402798, *2 (D. Mass. June 26, 2012) (Wolf, J.) (applying same standards in denying Rule 29 motion on venue, even where jury was not explicitly instructed on issue, because evidence viewed in the light most favorable to the verdict warranted conclusion that "jury implicitly found, based on adequate evidence, that venue was proper in Massachusetts").

Venue

Article III of the Constitution requires that criminal defendants "must be tried in the state or district in which the offense 'shall have been committed.'" *United States v. Seward*, 967 F.3d 57, 60 (1st Cir. 2020) (*quoting* U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI); *see also* Fed. R. Crim. P. 18 ("[T]he government must prosecute an offense in a district where the offense was committed."). Venue is analyzed separately for each count of an indictment. *United States v. Salinas*, 373 F.3d 161, 163 (1st Cir. 2004) (citing *United States v. Pace*, 314 F.3d 344, 349 (9th Cir. 1992)). "If the statute under which the defendant is charged contains a specific venue provision, that provision must be honored (assuming, of course, that it satisfies the constitutional minima)." *Salinas*, 373 F.3d at 164 (*citing Travis v. United States*, 364 U.S. 631, 635 (1961)); *see also United States v. Baugh*, 597 F. Supp. 3d 502, 507 (D. Mass. 2022) (Saris, J.) (same); *United States v. Abbas*, 2021 WL 784095, *3 (D. Mass. Mar. 1, 2021) (Sorokin, J.) (Fed. R. Crim. P. 18's venue requirements do not apply when "a statute ... permit[s] otherwise.").

Where an offense "span[s] multiple jurisdictions, or 'where a crime consists of distinct parts which have different localities[,] the whole may be tried where any part can be proved to have been done.'" *Seward*, 967 F.3d at 60 (citing *Rodriguez-Moreno*, 526 U.S. at 281). Continuing offenses that begin "in one district and [are] completed in another, or [are] committed

in more than one district, may be . . . prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237.

Only in the absence of specific venue guidance from Congress, *and* where an offense is not continuing, the "locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it." *Salinas*, 373 F.3d at 164. In making this determination, courts "identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." *United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999). In such instances, courts focus on "the conduct comprising the offense," but do not focus exclusively on "action verbs" in statutes to identify the conduct at issue. *Seward*, 967 F.3d at 61 (citations omitted). "[R]equiring the presence of an action verb to define the nature of the crime could sweep out conduct not enumerated by such action language but nonetheless essential to the offense." *Id.* (*citing Rodriguez-Moreno*, 526 U.S. at 280).

FACTS CONCERNING VENUE

On multiple occasions in October and November 2018, the defendant and his co-conspirators gained unauthorized access to DFIN's network using IP addresses that were part of a single IP address block beginning with the digits 104.238.37 ("the Boston 104 IPs"). Once inside the DFIN system, the hackers viewed and downloaded back to the server hosting the Boston 104 IPs the confidential earnings reports of dozens of companies, all using the stolen user credentials of DFIN employee Julie Soma. (*See, e.g.*, 1/31/23 Transcript ("Tr.") at 123-25 (testimony of Daron Hartvigsen that IP address in DFIN "download" logs was the IP address of the "unauthorized" "computer where that document would have gone") and 126 ("Q: And could you read the IP address that the download went to? A: 104.238.37.190").

The earnings reports accessed via the Boston 104 IPs using Soma's credentials included

those of dozens of publicly traded companies. (Ex. 191). The defendant and his co-conspirators traded in parallel in many of these stocks—consistently betting in the same direction, long on some, short on others. *Compare* Ex. 191 (summary of earnings report downloads using Julie Soma user ID from Boston 104 IPs), *with* Ex. 255 (summarizing parallel trading by defendant and other traders). Invariably, they placed their trades after the confidential earnings information was downloaded through the Boston 104 IPs, and unwound their positions following the subsequent public announcement of those earnings. *See, e.g.*, Exs. 199A–C (Capstead); 201A–C (Tesla); 258A–C (SSNC); 271A–C (Roku). With respect to Tesla, for example, the download to one of the Boston 104 IPs occurred at 5:18 a.m. on October 24, 2018. (Ex. 201B). Klyushin and co-conspirators Igor Sladkov and Mikail Irzak began buying later that same morning, while Rumiantcev followed later that same day. *Id.* The earnings were publicly announced after the market closed that afternoon, and the conspirators immediately sold their shares. *Id.*

The Boston 104 IPs to which the conspirators downloaded the MNPI belonged to an IP block assigned to Stackpath, a VPN service provider that operated through Strong Technology, IPVanish, and Mudhook Marketing, among other subsidiariers. The defendant's expert testified that VPN services offered subscribers an anonymous path to the internet. (2/9/23 Tr. at 44). The evidence showed that the Boston 104 IPs were assigned to a computer server located in a data center on Summer Street in Boston beginning in the spring of 2018 and continuing well into 2019:

- A former Stackpath director, Jacob Wall, testified that the Boston 104 IPs were located in Boston as of May 30, 2018, and that had they not been, his customers would have noticed degraded service and would have complained. Wall explained that Stackpath acquired the Boston 104 IPs from Web2Objects, an internet service provider, as part of Stackpath's expansion into the Boston market. Wall testified that upon leasing new IPs, his practice was to place them into immediate operation, to justify the expense. Stackpath subcontracted the work of installing the IPs on the Boston server to Micfo, a vendor Stackpath used throughout the country, which operated servers in the Boston data center, and which billed Stackpath for the service. Wall testified that he had never had any issues with Micfo and was satisfied with its work. 2/7/23 Tr. at 12-26.

- Wall's testimony was corroborated by: (1) a letter from Web2Objects, dated May 30, 2018, authorizing Micfo to install the Boston 104 IPs on a server in Boston; (2) a 2015 contract between Micfo and Markley Boston LLC for space in the Boston data center, pursuant to which Micfo paid Markley $950 per month; and (3) invoices from Micfo to Stackpath (through its Mudhook Marketing subsidiary) for the Boston server. (Exs 140 and 145). Although Wall was unable to locate invoices for the precise period spanning October 22 through November 8, 2018—the period when the downloads using Julie Soma's stolen login credentials occurred over those IPs—he testified that he had paid for the service well before then. And Stackpath's successor company did produce an invoice for the Boston 104 IPs dated November 24, 2018, which indicated that the IPs resided on a server in the Boston data center in space 7. (Ex. 140 at 5). A photograph dated September 13, 2018 showed a server in that location. Ex. 142D.

- A former Micfo network engineer, Aditi Shah, testified that on May 30, 2018—the same day Web2Objects issued the letter of authorization to Micfo—she transmitted it to Cogent Communications, the internet service provider for the Boston data center, and instructed Cogent to direct internet traffic to the Boston 104 IPs. (Ex. 267 at 6, 8). A Cogent customer support employee, Douglas Segura, replied later that same day that the task had "been completed." *Id.* at 1.

ARGUMENT

Count One – Conspiracy to Commit Unauthorized Access, Wire Fraud, and Securities Fraud

18 U.S.C. § 3237(a) provides that for a "continuing" offense, venue is proper "in any district in which such offense was begun, continued, or completed." "The classic example of a continuing offense is a conspiracy." *United States v. Yashar*, 166 F.3d 873, 875 (7th Cir. 1999); *United States v. McGoff*, 831 F.2d 1071, 1078 (D.C. Cir. 1987) (same). Accordingly, in a conspiracy prosecution, "it is clear beyond peradventure that venue [is] proper so long as any act in furtherance of the conspiracy was committed in the district. . . ." *United States v. Uribe*, 890 F.2d 554, 558 (1st Cir. 1989). A defendant need not even have been physically present in the district for venue to properly lie there. *Id.*; *United States v. Josleyn*, 99 F.3d 1182, 1191 (1st Cir. 1996) (same); *United States v. Sidoo*, 473 F. Supp. 3d 8, 12 (D. Mass. 2020) (same).

A rational jury could find that overt acts in furtherance of the conspiracy charged in Count One took place in Massachusetts. Repeatedly, in October and November 2018, one of the conspirators transmitted Julie Soma's username and password from the VPN server in Boston to DFIN's network—each time for the purpose of (1) obtaining unauthorized access to DFIN's network; (2) downloading valuable MNPI back to the Boston server for distribution to the conspirators; and (3) trading on the basis of the stolen information.

These overt acts, each of which was in furtherance of the conspiracy, amply support the jury's venue finding on Count One. *See United States v. Aurenheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (venue over conspiracy to violate Computer Fraud and Abuse Act "proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place"); *Josleyn*, 99 F.3d at 1191 ("venue in a conspiracy case depends upon whether an overt act in furtherance of the alleged conspiracy occurred in the trial district"); *United States v. Santiago*, 83 F.3d 20, 24-25 (1st Cir. 1996) ("single, overt act, taking place in Maine, is itself sufficient to sustain venue" over drug conspiracy). Moreover, because "[v]enue is also proper in any district through which electronic communications in furtherance of the conspiracy pass," *United States v. Mackey*, 2023 WL 363595, *7 (E.D.N.Y. Jan. 23, 2023), it matters little whether Klyushin used the Boston server as a "pass through"—as he contends—or as the launching point for his improper use of Julie Soma's credentials to access DFIN's servers, as the evidence shows.

Count Two – Wire Fraud, Aiding and Abetting

Section 3237 has particular applicability where, as here, "the use of modern communications facilities to execute a sophisticated criminal scheme inherently contemplates activities throughout many parts of the country." *United States v. Royer*, 549 F.3d 886, 893 (2d Cir. 2008); *see also United States v. Reed*, 773 F.2d 477, 480 (2d Cir. 1985) ("where the acts

constituting the crime and the nature of the crime charged implicate more than one location, the constitution does not command a single exclusive venue").

The defendant cannot dispute that wire fraud, like conspiracy, is a continuing offense. *See United States v. Carpenter*, 405 F. Supp. 2d 85, 91 (D. Mass. 2005), *aff'd in part, appeal dismissed in part*, 494 F.3d 13 (1st Cir. 2007) ("it is clear that to the extent a wire communication is sent from one district to or through one or more others, it also should be considered a 'continuing' offense, with venue proper in any district in which the offense was "begun, continued, or completed"). And a wire fraud offense is "continued" within the meaning of Section 3237 "if the wire transmission passes through facilities of interstate wire communication on its way from beginning to end." *Id.* Accordingly, courts in this District have repeatedly explained that "[i]n a wire fraud case, venue is established 'where the wire transmission at issue originated, *passed through*, or was received, or from which it was orchestrated. . . . '" *Foley*, 2013 WL 210187 at *1 (emphasis supplied) (*quoting Pace*, 314 F.3d at 349); *see also Abbas*, 2021 WL 784095 at *3 (same); *Harris*, 2012 WL 2402798 at *2 (same).

There is no dispute in this case that Julie Soma's username and password were repeatedly transmitted over the Boston 104 IPs to DFIN's servers, to gain unauthorized access to the DFIN computer network. Those wires—wherever they began, and wherever they were completed—plainly "continued" through Massachusetts. More is not required to establish venue for wire fraud under Section 3237. *See, e.g.*, *Carpenter*, 405 F. Supp. 2d at 91 (Massachusetts venue appropriate in wire fraud scheme for transaction that began in New Hampshire, cleared at the Federal Reserve Bank of Boston, and continued to a Merrill Lynch account in Pennsylvania); *United States v. Brown*, 293 F. App'x 826 (2d Cir. 2008) (wire fraud venue appropriate in district through which wire transfer related to fraud scheme passed, even though transfer was not processed in that

district); *United States v. Ebersole*, 411 F.3d 517 (4th Cir. 2005) (wire fraud venue appropriate in any district where the defendant "caused any payment-related wire communication to be transmitted").

But even if more were required, the evidence supplies it. The wires through Massachusetts were, as noted, essential to the scheme to steal valuable MNPI from DFIN. The defendant and his co-conspirators did not need Soma's username and password to access the Boston server from Russia; they needed her credentials to access DFIN's networks, which they did from the Boston server only after enlisting the anonymity of Stackpath's VPN connection. And the schemers did not use the Boston server solely to gain inbound access to DFIN; they also used it to receive the downloads of MNPI that they stole. Because the evidence established these Massachusetts acts in furtherance of the fraud scheme, the Court should deny defendant's motion as to Count Two.[1]

Count Three – Unauthorized Access to Computers, Aiding and Abetting

Count Three charged Klyushin with obtaining unauthorized access to a protected computer in furtherance of fraud, in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4). Although that statute does not contain a separate venue provision, Section 3237 provides that "*[a]ny offense* involving the use of the mails, *transportation in interstate or foreign commerce*, or the importation of an object or person into the United States is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce, mail matter, or imported

[1] It is of no moment whether Klyushin personally caused the wire transmission of Julie Soma's username and password from Massachusetts to Illinois. The jury's verdict holds him accountable for that transmission. *See Carpenter*, 405 F. Supp. 2d at 92 ("if Carpenter is properly held liable as a participant in the conduct of the scheme, many of the acts done in execution of that scheme occurred within Massachusetts, and venue is proper. This is one of those cases where the jury's guilty verdict necessarily implies a conclusion that venue for the trial of the charges against Carpenter was proper in Massachusetts.").

object or person moves." Accordingly, for the same reasons that the schemers' use of the Boston 104 IPs provided venue over the conspiracy and wire fraud offenses charged in Counts One and Two—insofar as the Boston IP address was the locus from which the schemers transmitted interstate wires to DFIN for the purpose of accessing its servers, and to which they received wires from DFIN transmitting stolen MNPI—venue is likewise appropriate over Count Three.

Moreover, even if the Court were to conclude that venue over the hacking offense depends on a determination of where the essential conduct elements of that crime lie, all of the statute's elements (other than the required *mens rea*) can be connected to Massachusetts: "First, that the defendant, or someone he aided and abetted, knowingly accessed without authorization a computer…"; . . . "Third, by accessing the computer without authorization, the defendant, or someone he aided and abetted, furthered the intended fraud"; and "Fourth, that the defendant, or someone he aided and abetted, by accessing the computer without authorization, obtained something of value." (2/10/23 Tr. at 126). Accessing without authorization and obtaining information have been held to be "essential conduct elements" of a violation of 18 U.S.C. § 1030(a)(2)(C), a CFAA provision that prohibits obtaining information through unauthorized access. *Aurenheimer*, 748 F.3d at 534. Where 18 U.S.C. § 1030(a)(4) prohibits accessing without authorization, furthering a fraud through that access, and obtaining something of value, it follows that each of these elements are "essential conduct elements" of a violation of this CFAA provision. Each requires a defendant's (or an aider and abetter's) action. They are clearly not "circumstance elements"—facts that existed at the times those actions are performed. *See United States v. Brennan*, 452 F. Supp. 3d 225, 234 (E.D. Pa. 2020). And, as the elements themselves make plain, the locations where the acts constituting the crime took place include, at a minimum, (1) where the defendant accessed a computer without authorization; (2) where the defendant furthered the

intended fraud; and (3) where the defendant obtained something of value.

As with each of the other counts of the Indictment, the offense charged in Count Three took place in several jurisdictions, including at least the following: (1) in Russia, where the defendant and his co-schemers were located and where they devised and initiated their scheme; (2) in Massachusetts, the jurisdiction where they accessed a VPN server to make it appear that the access to DFIN's computer network was coming from a domestic source, and to conceal their actual location and identity, from which they transmitted Julie Soma's stolen credentials to access to DFIN's servers, and to which they downloaded the stolen MNPI; (3) in Illinois, where DFIN's computers were located; and (4) in every other jurisdiction where the defendants accessed VPNs to serve as anonymizing platforms and launching pads for their attacks on the computer networks of DFIN and the schemers' other victim, Toppan Merrill.

Klyushin's citation to a thirteen-year-old DOJ manual on prosecuting computer crimes does nothing to advance his argument. As an initial matter, the internal guidelines of a federal agency, which are not mandated by statute or the constitution, do not confer substantive rights on any party. *See United States v. Michaud*, 860 F.2d 495, 497 (1st Cir. 1988); *United States v. Busher*, 817 F.2d 1409, 1411 (9th Cir. 1987) (defendant not entitled to rely on U.S. Attorneys' guidelines where manual stated it did not create any rights enforceable at law by any party). The preface to the manual Klyushin cites expressly states:

> The contents of this book provide suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any . . . criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 171 (1979).

It accordingly provides no legal basis for Klyushin's argument.

Moreover, a close reading of the manual undermines Klyushin's argument and supports venue in Massachusetts. Among other things, it notes that:

- the "Constitution and Rule 18 … leave questions unanswered in many network crime cases, such as how to define where an offense has been 'committed' or how to deal with crimes committed in multiple states or countries", and that "applying the principles of venue to network crimes is not always a straightforward endeavor";

- Multidistrict offenses "may be . . . prosecuted in any district in which such offense was begun, continued, or completed." (*quoting* 18 U.S.C. § 3237(a)); and

- "in today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused's actual presence" (*quoting United States v. Saavedra*, 223 F.3d 85, 86 (2d Cir. 2000)).

https://www.justice.gov/criminal/file/442156/download (visited Mar. 31, 2023), at 116-18.

Even the manual's hypothetical—of an intrusion originating in California, passing through an Arizona computer, which enabled unauthorized access to an Illinois computer, and obtaining information via that Illinois computer from a server in Kentucky—does not exclude Arizona as a proper venue. It notes that "venue is … proper at some, *if not all*, of the points in between [California and Kentucky], since venue may lie "in any district in which [a continuing] offense was begun, continued or completed." *Id.* at 118 (*citing* 18 U.S.C. § 3237(a)). "Under this section, the 'accessing' and 'obtaining' arguably continued in Arizona and Illinois." *Id.* at 118-19.

In this case, the transmission of Soma's credentials from Massachusetts to DFIN's computers in Illinois, in order to gain unauthorized access to the DFIN network, is the gravamen of the offense. Massachusetts is, accordingly, a place from which the defendant and his co-schemers furthered the fraud, and first obtained by download the MNPI—the thing of value that the statute requires. *United States v. Offill*, 2009 WL 1649777, *3 (E.D. Va. Jun. 10, 2009) (that spam emails related to fraudulent scheme passed through server located in district of prosecution was one factor in favor of retaining venue there). The commission of these essential conduct

elements here makes venue appropriate in Massachusetts, and the Court should deny the defendant's motion to acquit as to Count Three.

Count Four – Securities Fraud

The Securities Exchange Act of 1934 has its own venue provision, which provides in pertinent part that a "criminal proceeding may be brought in the district wherein any act or transaction constituting the violation occurred." 15 U.S.C. § 78aa. Acts sufficient to confer venue must "constitute" the securities fraud violation; "mere preparatory acts are insufficient." *See United States v. Khalupsky*, 5 F.4th 279, 291 (2d Cir. 2021), *cert. denied sub nom. Korchevsky v. United States*, 142 S. Ct. 761 (2022). "A securities fraud violation occurs where defendants 'use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device,' including the making of material false statements." *United States v. Lange*, 834 F.3d 58, 69 (2d Cir. 2016) (*quoting* 15 U.S.C. § 78j(b)).

Courts have consistently found that the transmission of fraudulent information is an appropriate basis for venue in securities fraud cases charged under Section 78. *See, e.g., Lange*, 834 F.3d at 72 (false statements directed by wire into district of prosecution were "crucial to the success of the scheme"); *United States v. Royer*, 549 F.3d 886, 894 (2d Cir. 2008) (venue proper in district from which manipulative communications "crucial to the success of the scheme" originated); *United States v. Johnson*, 510 F.3d 521, 525 (4th Cir. 2007) (transmission of fraudulent form to prosecuting venue was a "material act that constitutes the [securities fraud] violation").

Consistent with the securities fraud statute and these precedents, this Court properly instructed the jury that a securities fraud violation involves, among other elements, "employ[ing] any manipulative or deceptive device or contrivance; [or] any device, scheme or artifice to

defraud." 2/10/23 Tr. at 127–28. Likewise, the Court properly instructed the jury that, if "the scheme involved the defendant or another participant in the scheme misrepresenting his or her identity online to access computer systems to obtain material nonpublic information to trade on the confidential information," then it could "find that conduct [was] a deceptive device or contrivance, or a device, scheme or artifice to defraud within the meaning of the securities fraud statute." *Id*. at 129–30; *see also Khalupsky*, 5 F.4th at 291 ("[M]isrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly 'deceptive' within the ordinary meaning of the word."). Klyushin concedes that these instructions were correct. (Dkt. 222 at 2). He thus concedes that, in unanimously finding him guilty of securities fraud, the jury necessarily found that he and his co-schemers misrepresented their identities to gain access to DFIN's servers to obtain MNPI that they used to trade.

Instead, Klyushin challenges the jury's venue finding by simply asserting—without citing the applicable venue statute or any trial evidence (much less in the light most favorable to the government)—that the record "[a]t most . . . shows that Boston was a mere 'pass through' . . . an intermediate IP address assigned at random by a Virtual Private Network (VPN)." *Id.* at 3.

Klyushin's contention is unsupported, and falls far short of meeting his "daunting" burden. At trial, the evidence indisputably showed that the deceptive device or contrivance—the use of Julie Soma's password to access DFIN without authorization in order to obtain MNPI—occurred over the Boston 104 IPs.[2] And, as noted, the jury could rationally infer from the evidence that the

[2] It is irrelevant to venue whether the defendant himself, Ermakov, or another coconspirator used the Boston server to misrepresent himself as Julie Soma. *See Khalupsky*, 5 F.4th at 292 ("Once proper venue is established through [a co-schemer], it is enough that [the defendant] aided and abetted the scheme of securities fraud; we do[] not require that a defendant aid and abet the specific criminal activity occurring within the district of venue.").

defendant and his co-schemers did not need Julie Soma's credentials to access that Boston server. Indeed, the evidence showed that they utilized multiple *other* false identities—like "Andrea Neumann" and others—to purchase domain names and lease other computers that they used to hide their tracks and make it difficult to trace the hacks back to Russia. 2/2/23 Tr. at 123-31; 2/6/23 Tr. at 19-20; 2/7/23 Tr. at 144-45. But it was from the Boston server that they *directly* accessed DFIN's servers. And to access those DFIN servers, the conspirators needed to use the identity of a DFIN employee, Julie Soma. Using her credentials, they gained access to information that was otherwise off limits to them and stole it for the purpose of trading on it.

Nor were the misrepresentations over the Boston server "mere preparatory" acts, as in *United States v. Tzolov*, where the fact that the defendants simply traveled, via JFK Airport in Queens, to a meeting in a different district—where they ultimately made false statements—was insufficient to establish venue in the Eastern District of New York. 642 F.3d 314, 319 (2d Cir. 2011).[3] In contrast to this case, the defendants in *Tzolov* did not launch their false statements from the Eastern District—nor did they download the material nonpublic information to the Eastern District. Nor did they even use JFK Airport to conceal their identities and hide their scheme. Indeed, in that case, the Second Circuit found that a defendant's transmission of "any false or misleading information *into or out of* " the district of prosecution *would* provide a basis for venue on a securities fraud count. *See id.* at 318. Had the *Tzolov* defendants, for example, stopped while

[3] Even mere "preparatory acts" that would not satisfy the venue requirements of Section 78aa can still be overt acts that support venue in a securities fraud conspiracy. That is because an overt act "need not be unlawful; it can be any act, innocent or illegal, as long as it is done in furtherance of the object or purpose of the conspiracy." *See Tzolov*, 642 F.3d at 320 ("A reasonable jury could have concluded that [the defendants'] travel through the Eastern District was in furtherance of the conspiracy because, had they not done so, the face-to-face meetings with potential investors, which was a regular part of their fraudulent scheme, would not have occurred.").

at JFK to place a phone call in which they made false statements to their victims, or to change their appearance ahead of a meeting in which they would conceal their true identities, *that* behavior would have provided a basis for venue in the Eastern District of New York. And that is exactly what happened here: the schemers accessed a server in Boston, and then used that server anonymously to transmit Julie Soma's credentials out of Massachusetts to DFIN's servers, to gain unauthorized access to the MNPI, which they then viewed and downloaded back to the Boston server.

The Court should accordingly deny the motion to acquit as to Count Four.

Foreseeability

Retreating to a fallback argument, Klyushin also contends that the government failed to prove that he and his co-schemers "purposely availed themselves of a Boston-based IP address or consciously actuated its use – much less that the latter was within their knowledge or even reasonably foreseeable." Dkt. 222 at 3. But as this Court recognized when it declined to give a foreseeability instruction, there is no foreseeability requirement in the First Circuit, much less a requirement that the defendant have "purposefully availed" himself of the venue. *See* 2/8/23 Tr. at 26; *see also United States v. Sidoo*, 473 F. Supp. 3d 8, 14 (D. Mass. 2020) ("[T]he First Circuit has not adopted such a foreseeability requirement and several other circuits have explicitly rejected such a test in the context of section 3237(a). A foreseeability test is required by 'neither the text of the Constitution nor of § 3237(a)' and this Court will not adopt such a test.") (further citations omitted). The Court should decline the defendant's renewed invitation to establish a foreseeability requirement for venue, which at least three other circuits have refused to do. *See United States v. Renteria*, 903 F.3d 326, 329-30 (3d Cir. 2018) ("the Constitution and § 3237(a) focus solely on where the offense occurred and do not even reference foreseeability"); *United States v. Gonzalez*,

683 F.3d 1221, 1226 (9th Cir. 2012) ("[I]t does not matter whether [the defendant] knew or should have known that the CI was located in the Northern District of California during the calls. Simply put, section 3237(a) does not require foreseeability to establish venue for a continuous offense."); *Johnson*, 510 F.3d at 527 ("If Congress had wanted to limit venue to those districts where the defendant could have reasonably foreseen [the] criminal conduct taking place, it could have easily done so. Instead, it enacted a broad venue provision, one that lacked any reference to a defendant's mental state or predictive calculus. . . . ").

Moreover, even if—contrary to black-letter law—there were a foreseeability requirement to establish venue in this district, the evidence taken in the light most favorable to the government would plainly suffice to meet that hypothetical burden, as the Court has already suggested. *See* 2/8/23 Tr. at 180 ("[T]he merits of [foreseeability] do not favor the defense simply because if you're a hacker, you have to expect—I mean, that's the process, that there could be servers anywhere and that could be Massachusetts, but—so [I] certainly am not directing a verdict on that basis."). Indeed, the jury was rationally entitled to conclude from the evidence that the *whole purpose* of using anonymizing VPNs was to hide the schemers' location from their victims while lulling DFIN and TM into believing that the access to their networks was coming from legitimate sources within the United States. It was thus foreseeable to the defendant that those locations could be anywhere within the United States, including Massachusetts, as the Court noted. Where, as here, "the use of modern communications facilities to execute a sophisticated criminal scheme inherently contemplates activities throughout a large geographic area, conspirators should not then be able to escape the broad geographic scope stemming from the broad intentions of that scheme." *Royer*, 549 F.3d at 893; *see also Khalupsky*, 5 F.4th at 291-93 (vast scope of trading scheme and the defendants' expertise in trading made foreseeable the existence of counterparties in district of

prosecution). Contrary to Klyushin's suggestion, there is hardly "unfairness" and "hardship" in trying him here. (Dkt. 222 at 5). As the Court succinctly observed during the trial, "[i]f a hacker from somewhere outside the United States targets our computers or servers or companies here, I don't see that there's any difference in a venue or any additional hardship . . . as between Massachusetts or . . . Minnesota, [or] Chicago." (2/9/23 Tr. at 151). Defendant's failure to seek a different venue underscores the point that there was nothing uniquely unfair about trying a Russian national in Massachusetts for attacking U.S. computers from overseas. *See Gonzalez*, 683 F.3d at 1226 ("venue will often be possible in districts with which the defendant had no personal connection, and which may occasionally be distant from where the defendant originated the actions constituting the offense."); *United States v. Rommy*, 506 F.3d 108, 123 n.8 (2d Cir. 2007) (where Dutch defendant could not show that "being prosecuted in the Southern District of New York, as compared to some other United States venue … imposed an additional hardship on [him], prejudiced [him], or undermined the fairness of [his] trial . . ., no real constitutional venue concerns arise in this case"). The Court should, accordingly, deny the defendant's motion on this ground.

First Brought Venue Was Established for All Four Counts

The Court instructed the jury as to "first-brought" venue under 18 U.S.C. § 3238 only as to the conspiracy charge in Count One. 2/10/23 Tr. at 138. That instruction required the government to show by a preponderance of the evidence that "the offense was begun or committed outside of the United States," "that the defendant was first brought to the District of Massachusetts", and that "the essential conduct elements of the conspiracy took place outside the United States." *Id.* There is little dispute that the unlawful agreement charged in this case—to hack into the victims' computers, steal their MNPI, and trade on it—was hatched in Russia, where the defendant and all of his co-conspirators resided, and where the defendant's company, M-13,

was located. That same criminal conspiracy was complete, as a matter of law, as soon as Klyushin or any of his associates committed a single overt act in furtherance of any one of its objects—such as by using M-13's infrastructure to lease virtual servers and domains used in the attack, or by transmitting any of the myriad encrypted communications they sent to each other discussing their plot. And the defendant stipulated that, following his arrest in Switzerland, he was brought directly to Boston. Accordingly, a rational jury could easily conclude, as the jury here plainly did, that (1) the conspiracy was begun outside the United States, (2) the conspiracy was also committed outside the United States insofar as the "essential conduct elements" took place in Russia, and (3) the defendant was first brought to Massachusetts after his arrest, thereby satisfying the venue requirements of Section 3238.

The government further contends, for the reasons stated in its briefing to the Court on first-brought jurisdiction—which it incorporates here by reference, *see* Dkts. 192 and 195—that Section 3238 also provided a proper basis for venue on Counts Two, Three, and Four. Those crimes were each "begun" outside the United States, for the same reasons that the conspiracy was begun there. Moreover, because Section 3238 is silent on "essential conduct" elements in the context of crimes begun abroad, its requirements are satisfied without regard to where the essential conduct elements of those crimes were committed. *See United States v. Miller*, 808 F.3d 607, 619 (2d Cir. 2015) (language "begun or committed" out of the jurisdiction of any particular state suggests "that the statute encompasses offenses 'begun' outside the borders of the United States—but ending within our country's borders").[4]

[4] Here, in any event, Count Two, charging wire fraud, was also committed and completed outside the United States, insofar as the defendant and his co-schemers sent numerous communications and other wires in furtherance of the scheme outside the United States.

CONCLUSION

This Court went to great lengths to ensure that Klyushin received a fair trial in Massachusetts, and a unanimous jury convicted him on all counts based on evidence that was overwhelming. Klyushin's Rule 29 motion does not seriously dispute either of those conclusions. Further, Klyushin was properly tried in Massachusetts. For the reasons set forth above, the government met its burden of establishing venue by a preponderance of the evidence, especially when the evidence and reasonable inferences from that evidence are taken in the light most favorable to the government, as they must be in the context of a Rule 29 motion. The Court should, accordingly, deny the defendant's motion.

Respectfully submitted,

RACHAEL S. ROLLINS
United States Attorney

By: */s/ Seth B. Kosto*
STEPHEN E. FRANK
SETH B. KOSTO
Assistant U.S. Attorneys

Date: March 31, 2023

CERTIFICATE OF SERVICE

I hereby certify that a copy of this document will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Seth B. Kosto
SETH B. KOSTO
Assistant U.S. Attorney

Date: March 31, 2023